How to Delegate Computations: The Power of No-Signaling Proofs

Ran Raz
(Weizmann Institute & IAS)

Joint work with:
Yael Tauman Kalai
Ron Rothblum
Delegation of Computation
Delegation of Computation:

Alice has $x \in \{0,1\}^n$

Alice needs to compute $f(x)$, where $f$ is publicly known

Bob offers to compute $f(x)$ for Alice

Alice sends $x$ to Bob

Bob sends $f(x)$ to Alice

\[ f(x) \]
1-Round Delegation Scheme for $f$:

1) Completeness: if $P$ is honest:
   \[ \Pr[V \text{ accepts}] = 1 - \neg \]

2) Soundness: $\forall P^* \in \text{Time}[t^*(n)]$, if $b \neq f(x)$:
   \[ \Pr[V \text{ rejects}] = 1 - \neg \]

3) Running time of $P$: $\text{poly}(t(n))$

4) Running time of $V$: $\ll t(n)$

$f \in \text{Time}[t(n)]$
Previous Work [GKR+KR]:

If \( f \) is a logspace-uniform circuit of size \( t \) and depth \( d \):

1-round delegation scheme s.t.:

Running time of \( P \): \( \text{poly}(t) \)

Running time of \( V \): \( O(n + \text{poly}(d)) \)

(under exponential hardness assumptions)
Our Result:

If $f \in \text{Time}[t(n)]$

1-round delegation scheme s.t.:

Running time of $P$: $\text{poly}(t(n))$

Running time of $V$: $n \cdot \text{polylog}(t(n))$

(under exponential hardness assumptions)
Variants of Delegation Schemes:

1-Round or Interactive
Computational or Statistical soundness:

- 1-Round, Computational: This talk!
- 1-Round, Statistical: Impossible!
- Interactive, Computational: Solved! (with only 2-rounds) [Killian, Micali],
  (based on $\text{MIP} = \text{NEXP}$) [BFL]
- Interactive, Statistical: [GKR 08]

- Many other works, under unfalsifiable assumptions, or with preprocessing.
The Approach of Aiello et al.
2-Prover Interactive Proofs [BGKW]:
Provers $A, B$ claim that $x \in L$
$V$ sends a query $q$ to $A$ and $r$ to $B$
no communication between $A$ and $B$
$A$ answers by $a = A(q)$
$B$ answers by $b = B(r)$
$V$ decides accept/reject by $q, r, a, b$
MIP=\textit{NEXP} (scaled down) \textbf{[BFL+FL]}:

\[ \forall L \in \text{Time}[t(n)], \exists \text{2-provers MIP s.t.} \]

1) Completeness: if \( A,B \) are honest:
   \[ \text{Pr}[V \text{ accepts}] = 1 \]

2) Soundness: \( \forall A \uparrow^*, B \uparrow^* \text{ if } x \notin L: \)
   \[ \text{Pr}[V \text{ rejects}] = 1 - \text{neg} \]

3) Running time of \( A,B: \text{ poly}(t(n)) \)

4) Running time of \( V: O(n) \)

5) Communication: \( \text{polylog}(t(n)) \)
[Aiello Bhatt Ostrovsky Sivarama 00]:

MIP $\Rightarrow$ 1-Round Argument ?!

MIP:

$q, r = \text{FHE of } q, r \text{ (with different keys)}$

$a, b = \text{FHE of } a = A(q), b = B(r)$
No-Signaling Strategies:

\[ a = A(q,r,z), \quad b = B(q,r,z) \]

(where \( z \) is a shared random string):

Given \( q \), the random variables \( a, r \)
are independent

Given \( r \), the random variables \( b, q \)
are independent
No-Signaling Strategies for $k$ provers: queries $q_{\downarrow 1}, \ldots, q_{\downarrow k}$, answers $a_{\downarrow 1}, \ldots, a_{\downarrow k}$

$$a_{\downarrow i} = A_{\downarrow i}(q_{\downarrow 1}, \ldots, q_{\downarrow k}, z), \quad (z = \text{random string})$$

For every $S \subseteq [k]$: Given $\{q_{\downarrow i} : i \in S\}$, $\{a_{\downarrow i} : i \in S\}$, $\{q_{\downarrow i} : i \notin S\}$, are independent

Soundness Against No-Signaling:

$$\forall \text{no-signaling} \ (A_{\downarrow 1}, \ldots, A_{\downarrow k}) \uparrow^*, \quad \text{if } x \notin L: \quad \Pr[V \text{ rejects}] = 1 - \text{neg}$$
We Show (using [ABOS 00]):

MIP with no-signaling soundness $\implies$ 1-Round Argument

(we need soundness for almost-no-signaling strategies)

Corollary:

Interactive Proof $\implies$ 1-Round Argument

(under exponential hardness assumptions)

Gives a simpler proof for [KR 09]

Challenge: Show stronger MIPs with no-signaling soundness
No-Signaling Strategies
Entangled Strategies: \( A, B \) share entangled quantum state \( |s_i\rangle_{A, B} \)

- \( A \) gets \( q \), \( B \) gets \( r \)
- \( A \) measures \( A \), \( B \) measures \( B \)
- \( A \) answers \( a \), \( B \) answers \( b \)

Soundness Against Entangled Strategies:
\[
\forall \text{entangled } (A\downarrow 1, \ldots, A\downarrow k)^{\uparrow \ast}, \text{ if } x \notin L:
\Pr[V \text{ rejects}] = 1 - \text{neg}
\]
Entangled vs. No-Signaling:

Entangled strategies are no-signaling

Signaling $\Rightarrow$ information travels faster than light

Hence, no-signaling is likely to hold in any future ultimate theory of physics

No-signaling soundness is likely to ensure soundness in any future physical theory
MIPs with No-Signaling Soundness:

No-Sig cheating provers are powerful:
\[ \text{PSPACE} \subseteq \text{no-sig MIP} \subseteq \text{EXP} \]
\[ \text{no-sig MIP}(2) = \text{PSPACE} \] (by linear programing)

In particular, all known protocols for \( \text{MIP} = \text{NEXP} \) are not sound for no-signaling

Example: Assume: \( V \) checks \( a \oplus b = v \downarrow q, r \)
Let \( a = v \downarrow q, r \oplus z \). Let \( b = z \). (\( z \) is random)
Then \( V \) always accepts.
Our Result: \( \text{no-sig MIP} = \text{EXP} \)

If \( L \in \text{Time}[t(n)] \), MIP s.t.:

Running time of \( P \downarrow 1, \ldots, P \downarrow k \) :
\[ \text{poly}(t(n)) \]

Running time of \( V \) :
\[ O(n) \]

Number of provers: \( k = \text{polylog}(t(n)) \)

Communication: \( \text{polylog}(t(n)) \)

Completeness: 1

Soundness: against no-sig strategies
(with negligible error)

(gives soundness against entangled provers)
Delegating Computation to the Martians:
Delegating Computation to the Martians:

$L \in \text{Time}[t(n)]$

Running time of provers: $\text{poly}(t)$

Running time of $V$: $O(n)$

Number of provers: $k = \text{polylog}(t)$

Number of provers: $\text{polylog}(t)$

Completeness: 1

Soundness: against no-sig strategies (with negligible error)
Steps of the Proof
No-Signaling PCPs:
For every subset $S$ of locations s.t. $|S| \leq K$, $\exists$ distribution $A \downarrow S$
If $V$ queries locations $S = \{ q \downarrow 1, \ldots, q \downarrow d \}$, the answers are given by $(a \downarrow 1, \ldots, a \downarrow d) \in \downarrow R$
$A \downarrow S$

Guarantee: if $|S \downarrow 1|, |S \downarrow 2| \leq K$, then $A \downarrow S \downarrow 1, A \downarrow S \downarrow 2$ agree on their intersection

Step I: Switch to PCP: PCP with no-sig soundness implies $MIP$ with no-sig soundness, with $O(K)$ provers
Our Result:

\[ L \in \text{Time}[t(n)] \quad \text{PCP s.t.:} \]

Running time of prover: \(\text{poly}(t)\)

Running time of \(V\): \(O(n)\)

Number of queries: \(\text{polylog}(t)\)

Completeness: 1

Soundness: against no-sig strategies with \(K = \text{polylog}(t)\) (with negligible error)
Thank You!